

The NHS Standard Contract 2019-20 includes the following General Conditions (GC):

GC21 Patient Confidentiality, Data Protection, Freedom of Information and Transparency

Information Governance – General Responsibilities

21.1 The Parties must comply with Data Protection Legislation, Data Guidance, the FOIA and the EIR, and must assist each other as necessary to enable each other to comply with these obligations.

21.2 The Provider must complete and publish an annual information governance assessment in accordance with, and comply with the mandatory requirements of, the NHS Data Security and Protection Toolkit, as applicable to the Services and the Provider's organisation type.

21.3 The Provider must:

21.3.1 nominate an Information Governance Lead;

21.3.2 nominate a Caldicott Guardian and Senior Information Risk Owner, each of whom must be a member of the Provider's Governing Body;

21.3.3 where required by Data Protection Legislation, nominate a Data Protection Officer;

21.3.4 ensure that the Co-ordinating Commissioner is kept informed at all times of the identities and contact details of the Information Governance Lead, Data Protection Officer, Caldicott Guardian and the Senior Information Risk Owner; and

21.3.5 ensure that NHS England and NHS Digital are kept informed at all times of the identities and contact details of the Information Governance Lead, Data Protection Officer, Caldicott Guardian and the Senior Information Risk Owner via the NHS Data Security and Protection Toolkit.

21.4 The Provider must adopt and implement the National Data Guardian's Data Security Standards and must comply with further Guidance issued by the Department of Health and Social Care, NHS England and/or NHS Digital pursuant to or in connection with those standards. The Provider must be able to demonstrate its compliance with those standards in accordance with the requirements and timescales set out in such Guidance, including requirements for enabling patient choice.

21.5 The Provider must, at least once in each Contract Year, audit its practices against quality statements regarding data sharing set out in NICE Clinical Guideline 138.

21.6 The Provider must ensure that its NHS Data Security and Protection Toolkit submission is audited in accordance with Information Governance Audit Guidance where applicable. The Provider must inform the Co-ordinating Commissioner of the results of each audit and publish the audit report both within the NHS Data Security and Protection Toolkit and on its website.

21.7 The Provider must report and publish any Data Breach and any Information Governance Breach in accordance with IG Guidance for Serious Incidents. If the Provider is required under Data Protection Legislation to notify the Information Commissioner or a Data Subject of a Personal Data Breach then as soon as reasonably practical and in any event on or before the first such notification is made the Provider must inform the Co-ordinating Commissioner of the Personal Data Breach. This GC21.7 does not require the Provider to provide the Co-ordinating Commissioner with information which identifies any individual affected by the Personal Data Breach where doing so would breach Data Protection Legislation.

Data Protection

21.8 The Provider must have in place a communications strategy and implementation plan to ensure that Service Users are provided with, or have made readily available to them, Privacy Notices, and to disseminate nationally-produced patient information materials. Any failure by the Provider to inform Service Users as required by Data Protection Legislation or Data Guidance about the uses of

Personal Data that may take place under this Contract cannot be relied on by the Provider as evidence that such use is unlawful and therefore not contractually required.

21.9 Whether or not a Party or Sub-Contractor is a Data Controller or Data Processor will be determined in accordance with Data Protection Legislation and the ICO Guidance on Data Controllers and Data Processors and any further Data Guidance from a Regulatory or Supervisory Body. The Parties acknowledge that a Party or Sub-Contractor may act as both a Data Controller and a Data Processor. The Parties have indicated in the Particulars whether they consider the Provider to be a Data Processor on behalf of one or more of the Commissioners for the purposes of this Contract.

21.10 The Provider must ensure that all Personal Data processed by or on behalf of the Provider in the course of delivering the Services is processed in accordance with the relevant Parties' obligations under Data Protection Legislation and Data Guidance.

21.11 In relation to Personal Data processed by the Provider in the course of delivering the Services, the Provider must publish, maintain and operate:

21.11.1 policies relating to confidentiality, data protection and information disclosures that comply with the Law, the Caldicott Principles and Good Practice;

21.11.2 policies that describe the personal responsibilities of Staff for handling Personal Data;

21.11.3 a policy that supports the Provider's obligations under the NHS Care Records Guarantee;

21.11.4 agreed protocols to govern the sharing of Personal Data with partner organisations; and

21.11.5 where appropriate, a system and a policy in relation to the recording of any telephone calls or other telehealth consultations in relation to the Services, including the retention and disposal of those recordings, and apply those policies and protocols conscientiously.

21.12 Where a Commissioner requires information for the purposes of quality management of care processes, the Provider must consider whether the Commissioner's request can be met by providing anonymised or aggregated data which does not contain Personal Data. Where Personal Data must be shared in order to meet the requirements of the Commissioner, the Provider must:

21.12.1 provide such information in pseudonymised form where possible; and in any event

21.12.2 ensure that there is a legal basis for the sharing of Personal Data.

21.13 Notwithstanding GC21.12, the Provider must (unless it can lawfully justify non-disclosure) disclose defined or specified confidential patient information to or at the request of the Co-ordinating Commissioner where support has been provided under the Section 251 Regulations, respecting any individual Service User's objections and complying with other conditions of the relevant approval.

The Provider as a Data Processor

21.14 Where the Provider, in the course of delivering the Services, acts as a Data Processor on behalf of a Commissioner, the provisions of Schedule 6F (*Provider Data Processing Agreement*) will apply.

Responsibilities when engaging Sub-Contractors

21.15 Subject always to GC12 (*Assignment and Sub-Contracting*), if the Provider is to engage any Sub-Contractor to deliver any part of the Services (other than as a Data Processor) and the Sub-Contractor is to access personal or confidential information or interact with Service Users, the Provider must impose on its Sub-Contractor obligations that are no less onerous than the obligations imposed on the Provider by this GC21.

21.16 Without prejudice to GC12 (*Assignment and Sub-Contracting*), if the Provider is to require any Sub-Contractor to act as a Data Processor on its behalf, the Provider must:

21.16.1 require that Sub-Contractor to provide sufficient guarantees in respect of its technical and organisational security measures governing the data processing to be carried out, and take reasonable steps to ensure compliance with those measures;

21.16.2 carry out and record appropriate due diligence before the Sub-Contractor processes any Personal Data in order to demonstrate compliance with Data Protection Legislation; and

21.16.3 as far as practicable include in the terms of the sub-contract terms equivalent to those set out in Schedule 6F (*Provider Data Processor Agreement*) and in any event ensure that the Sub-Contractor is engaged under the terms of a binding written agreement requiring the Sub-Contractor to:

21.16.3.1 process Personal Data only in accordance with the Provider's instructions as set out in the written agreement, including instructions regarding transfers of Personal Data outside the EU or to an international organisation unless such transfer is required by Law, in which case the Data Processor shall inform the Provider of that requirement before processing takes place, unless this is prohibited by law on the grounds of public interest;

21.16.3.2 ensure that persons authorised to process the Personal Data on behalf of the Sub-Contractor have committed themselves to confidentiality or are under appropriate statutory obligations of confidentiality;

21.16.3.3 comply at all times with those obligations set out at Article 32 of the GDPR and equivalent provisions implemented into Law by DPA 2018;

21.16.3.4 impose obligations as set out in this GC21.16.3 on any Sub-processor appointed by the Sub-Contractor;

21.16.3.5 taking into account the nature of the processing, assist the Provider by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Provider's obligation to respond to requests for exercising rights granted to individuals by Data Protection Legislation;

21.16.3.6 assist the Provider in ensuring compliance with the obligations set out at Article 32 to 36 of the GDPR and equivalent provisions implemented into Law, taking into account the nature of processing and the information available to the Sub-Contractor;

21.16.3.7 at the choice of the Provider, delete or return all Personal Data to the Provider after the end of the provision of services relating to processing, and delete existing copies unless the Law requires storage of the Personal Data;

21.16.3.8 create and maintain a record of all categories of data processing activities carried out under the Sub-Contract, containing:

21.16.3.8.1 the name and contact details of the Data Protection Officer (where required by Data Protection Legislation to have one);

21.16.3.8.2 the categories of processing carried out on behalf of the Provider;

21.16.3.8.3 where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards; and

21.16.3.8.4 a general description of the technical and organisation security measures taken to ensure the security and integrity of the Personal Data processed under this Contract;

21.16.3.9 guarantee that it has technical and organisational measures in place that are sufficient to ensure that the processing complies with Data Protection Legislation and ensures that the rights of Data Subject are protected;

21.16.3.10 allow rights of audit and inspection in respect of relevant data handling systems to the Provider or to the Co-ordinating Commissioner or to any person authorised by the Provider or by the Co-ordinating Commissioner to act on its behalf; and

21.16.3.11 impose on its own Sub-Contractors (in the event the Sub-Contractor further sub-contracts any of its obligations under the Sub-Contract) obligations that are substantially equivalent to the obligations imposed on the Sub-Contractor by this GC21.16.3.

21.17 The agreement required by GC21.16 must also set out:

21.17.1 the subject matter of the processing;

21.17.2 the duration of the processing;

21.17.3 the nature and purposes of the processing;

21.17.4 the type of personal data processed;

21.17.5 the categories of data subjects; and

21.17.6 the plan for return and destruction of the data once processing is complete unless the Law requires that the data is preserved.

Freedom of Information and Transparency

21.18 The Provider acknowledges that the Commissioners are subject to the requirements of FOIA and EIR. The Provider must assist and co-operate with each Commissioner to enable it to comply with its disclosure obligations under FOIA and EIR. The Provider agrees:

21.18.1 that this Contract and any other recorded information held by the Provider on a Commissioner's behalf for the purposes of this Contract are subject to the obligations and commitments of the Commissioner under FOIA and EIR;

21.18.2 that the decision on whether any exemption under FOIA or exception under EIR applies to any information is a decision solely for the Commissioner to whom a request for information is addressed;

21.18.3 that where the Provider receives a request for information relating to the Services provided under this Contract and the Provider itself is subject to FOIA or EIR, it will liaise with the relevant Commissioner as to the contents of any response before a response to a request is issued and will promptly (and in any event within 2 Operational Days) provide a copy of the request and any response to the relevant Commissioner;

21.18.4 that where the Provider receives a request for information and the Provider is not itself subject to FOIA or as applicable EIR, it will not respond to that request (unless directed to do so by the relevant Commissioner to whom the request relates) and will promptly (and in any event within 2 Operational Days) transfer the request to the relevant Commissioner;

21.18.5 that any Commissioner, acting in accordance with the codes of practice issued and revised from time to time under both section 45 of FOIA and regulation 16 of EIR, may disclose information concerning the Provider and this Contract either without consulting with the Provider, or following consultation with the Provider and having taken its views into account; and

21.18.6 to assist the Commissioners in responding to a request for information, by processing information or environmental information (as the same are defined in FOIA or EIR) in accordance with a records management system that complies with all applicable records management recommendations and codes of conduct issued under section 46 of FOIA, and providing copies of all information requested by that Commissioner within 5 Operational Days of that request and without charge.

21.19 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of FOIA, or for which an exception applies under EIR, the content of this Contract is not Confidential Information.

21.20 Notwithstanding any other term of this Contract, the Provider consents to the publication of this Contract in its entirety (including variations), subject only to the redaction of information that is exempt from disclosure in accordance with the provisions of FOIA or for which an exception applies under EIR.

21.21 In preparing a copy of this Contract for publication under GC21.20 the Commissioners may consult with the Provider to inform decision-making regarding any redactions but the final decision in relation to the redaction of information will be at the Commissioners' absolute discretion.

21.22 The Provider must assist and cooperate with the Commissioners to enable the Commissioners to publish this Contract.